Public Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects under the GDPR

Response to questions for public consultation by [redacted]

The answers below correspond with the questions set out in the consultation document

1. It is vital that methods are found which allow organisations that collect and use children's personal data clearly and straightforwardly to explain to children what they do with these data, what tools are available to them to correct or erase the data, and what their rights are to redress.

   The obligation to disclose should extend to disclosure of any inferences which a company has drawn based on its analysis of any data which describes or records an individual's behaviour.

   It is impossible for parents or teachers to explain to children how this might work if different organisations use different language and approaches. We therefore strongly recommend the DPC sets out a standard approach by which organisations can communicate with children. This could be hosted on the DPC site where it could be easily found. The Open Rights Group in the UK appear to have done something along these lines in respect of financial institutions. In Germany a Guideline exists for providers of web services particularly addressed to children (https://www.kinderrechte.digital/hintergrund/index.cfm/topic.324/key.1578)

   An added benefit is this ought to ease the task of comparing data processing practices across organisations so that, for instance, NGOs or child rights organisations could compare approaches in order to identify good and poor practice, and work towards improvements.

   It is important to find ways to include all organisations which process children's data, including those such as Oracle or Experian or other third-party operators which operate as data collectors or brokers "behind the scenes". We say this because it appears as if it is becoming increasingly common for, for example, social media sites to obtain information from third parties and integrate it into a user's profile even though the user in question has not rendered it to the site via the mechanism of the App under consideration.

The challenge, as ever, is to find appropriate and proportionate ways or methods which work in the context of the particular application, web site or other online service under consideration.

In relation to transparency and explaining what information is being collected and how it is used, much will depend on the levels of literacy and understanding of each account holder. However, without using potentially hugely intrusive data collection practices this presents businesses with a dilemma or a problem. While they must have a sound, research-based understanding of who their customers are, inevitably businesses will be forced to develop approaches which work with broad categories of children, using age as the denominator.

A layered approach seems sensible. With younger children one would expect greater use to be made of graphics, cartoons or pictograms and additional audio and video files which convey the essence of the messages whereas with older children a greater reliance on or use of accessible text is likely to be acceptable.

2. Ideally one would be able to find a single way that worked to convey all the essential information effectively to all relevant audiences, perhaps allowing for links to be provided for anyone who wished to scrutinise the legal or technical minutiae of every policy. Failing that companies should use separate sets of transparency information, tailored for each audience. In multi lingual societies this will be necessary in any event.
3. At any age. If a child is capable of making such a request, they should be answered properly, as is their right. We cannot think of any or at any rate many circumstances where it would be appropriate for an online business or app provider to deny a person, whatever their age, access to data about themselves where they had generated and therefore "owned" it. Perhaps there could be a limited and temporary exception where a police investigation or other legal action arose where the processes required some restriction or limitation to be applied.
4. Each case should be judged on the facts with the starting position being that the data belongs to the child alone.
   Ordinarily the parent therefore has no right of access. A coercive parent might bully or manipulate a child into making a joint application but, in reality, it may not be in the child's best interests for the parent to be able to access the data. However, the company itself is unlikely to be a trusted arbiter in such cases. For that reason an online business might consider establishing a process or procedure for evaluating both joint applications and applications that came from the parent alone. Applications from the parent alone could be legitimate where there are genuine grounds for concern about a child's well- being. When considering applications from the parent alone or a joint application it is likely the business will benefit from having a degree of independent, expert advice.
5. See above.
6. At any age. If a child is capable of making such a request, they should be answered properly, as is their right. We cannot think of any or at any rate many circumstances where it would be appropriate for an online business or app provider to deny any child the right of erasure in respect of data about themselves where they had generated and therefore "owned" it. Perhaps there could be a limited and temporary exception where a police investigation or other legal action arose where the processes required some restriction or limitation to be applied.

7. Our answer here is similar to our answer to 4. Each case should be judged on the facts with the starting position being that ordinarily only the child has the locus to exercise a right of erasure in respect of their data. However, there may be circumstances where it is in a child's best interests for data to be erased and the parents should have the power to be able to make the request. However, the company itself is unlikely to be a trusted arbiter in such cases. For that reason an online business might consider establishing a process or procedure for evaluating such applications to ensure it can benefit from independent expert advice.
8. It has not been possible for us to answer this question as we are not aware of the data sources that might be available to assist with an age verification process in Ireland. However, principally it will be the responsibility of the DPC to determine the adequacy of the approach.
9. See answer to question 8.
10. Logically, "yes" if the applicable law is the law of Ireland. However, Irish law may not be the applicable law in every case where an end user lives in or is using the service in Ireland.
11. They need to determine which is the applicable law for each user and make sure they comply with it. The age limits for each jurisdiction are known and it therefor ought to be a relatively easy technical task to match geo-location data with appropriate terms and conditions.
12. The degree of risk of harm likely to attach to the individual concerned in relation to the particular product or service being advertised, promoted or provided for example so-called "beauty surgery" or dietary products which raise both ethical and safety concerns.
13. The GDPR says that ordinarily children should not be the subject of profiling and that, in any event, any use of profiling must be based on a risk assessment. Given the inherent difficulties of doing this within the limitations of current technologies, the crudeness of the available tools, we urge that, until more reliable techniques become available, there should be a blanket ban on all profiling where the entity concerned is commercial in nature.
14. We urge that the DPC develops a widely trusted and reliable kite marking or licencing system, similar to that which exists in relation to electrical and electronic products, which certifies that a particular product or service met certain minimum safety and privacy standards (subject to independent oversight) and no product or service can be sold or supplied to the Irish market without such a licence or kitemark. It is likely that such a system would be more likely to succeed if it was operated at EU level with the backing of an EU institution.
15. I) Yes. II) Yes III) The product or service should be able to trigger changes automatically as the user passes stated age milestones.
16. We believe there has been excessive and unfair use made of "legitimate interests" as the basis of collecting and processing children's data. In effect this has reduced or excluded the scope for parental engagement with their children's online lives. It has also generated widespread confusion among the public. Even though within the narrow, legalistic scope of the GDPR one might be engaging on the basis of legitimate interest, to the average person there is an implication that you are consenting to that arrangement, but nobody clearly explains that this is not the case nor the consequences of it.

    Crucially, we consider it unacceptable that organisations have opted to use one or other of the provisions of Article 6 driven by financial or business considerations rather than by concerns about what is likely to be in the best of interests of children. The provisions of Article 6 being relied on can vary from jurisdiction to jurisdiction even for the same App. That cannot be right. Thus in the UK where the Article 8 age of consent is 13 a 13 year old

can join on the basis of giving their consent. In another jurisdiction, for the same App, a 13 year old can join a slightly different version on the basis of legitimate interests even though a consent provision also exists, though it requires parental consent. Such obvious inconsistencies undermine public trust and understanding, and it is hard to see how they might have been driven by what is likely to be in the best interests of children.

---ooo---

1st March 2019